Result Page

Notice: This translation is produced by an automated process; it is intended only to make the technical content of the original document sufficiently clear in the target language. This service is not a replacement for professional translation services. The esp@cenet® Terms and Conditions of use are also applicable to the use of the translation tool and the results derived therefrom.

2,1 technical field

Access supervision on electronic stored, confidential and schutzbedüftige data in distributed and heterogeneous environment, in particular also in the Internet

2,2 state of the art

The represented invention develops essentially on the technology of the Internet as well as cryptographic methods, thus such, which use digital encryption and signature.

As far as possible, respect taken becomes, the z the state of the art on the RFC recognized in the Internet ("Request For Comments"). B. bottom http://www.rfc-editor.org is callable. This RFC fulfill on the one hand the function of recognized standards, on the other hand one they serve also for the technical discussion, so that new developments find here early their precipitation

2.2.1 Internet protocols

2.2.1.1 TCP/IP

The backbone of the Internet forms a standardized group of network communication protocols, which become frequent the bottom contraction "TCP/IP" summarized however in broad senses to also contain:

- The "Internet Protocol" (IP, [RFC 791]) points in the Internet an unique address to each computer from 4 bytes to (typical notation 123.234.56.78) several computers can Subnetzen summarized become.
The data transfer made in packets (type. approx. 1 kByte large) interface computers ("routers") take over as exchanges the connection between Subnetzen. If a packet over

several Subnetze must become away transported, it is passed on from router to router. Normally is to be assumed neither transmitters nor receivers possess the control over all routers and Subnetze of the transmission link. Therefore the Internet is considered as inherent uncertainly and susceptibly to hearing and falsifying data as well as wrong identity statements ("IP-Spoofing")
A new version of the Internet protocol (IP-V6, see [RFC 1883]) is in preparation, has itself however not yet established in the practice.
- The "Transmission Control Protocol" (TCP, [RFC 793]) puts the hidden packet transmission on before the application programmes on IP and. An application requests a connection from TCP to a certain computer (identified over the IP address). TCP makes the applications "Sockets", a pair of interfaces available, over which sequentially data read and written to become to be able. This Sockets corresponds with those at the receiving station, so that the applications on both computers can communicate over this Socket pair, without worrying about the underlying network structure.
In order to let at a computer various programmes (or several instances of the same program) develop independently connections, included TCP a "port address", some certain Socket of if necessary. several on a computer to identify can.
- "User the datagram Protocol" (UDP, [RFC 768]) is a somewhat simpler alternative to TCP and touches down likewise on IP. UDP knows no connections such as TCP, but sends arbitrary prolonged data sequences ("datagrams") to the receiving station, without waiting for an acknowledgment. UDP hidden thereby above all the network layer and the package structure.
Also UDP knows, like TCP, several port on a computer.
- The Domain namesystem (DNS, see [RFC 1034)/[RFC 1035]) the possible allocation from network addresses to easy stamping seed name (typical notation: host.org anisation.land) and the overlay of an organizational aligned arrangement of the network over the technical structure of the IP address with the Sub networks.
The DNS system is designed as distributed database with many buffers. Thus it (with correct configuration) becomes however susceptible very stable, to abuse by conscious false configuration ("DNS Spoofing") in limited net segments.

2.2.1.2 universal resource Locators

Universal arrange resource Locators (URL [RFC 1738]) each network resources (z. B. Computer, Mail account, text file, image file, clay/tone file) a stringer too, over which the resource in the Internet can become achieved. URL contain typically used application minutes, the server which can be addressed and if necessary. other informations for the specification of the resource relative to the server.

The concept of the URL became universal in the current valid standard "resource the Identifier" (URI, [RFC 2396]) extended, that beyond the net accessibility resources unique identified.

URL can identify also a programme or an Program interface. In this case it can contain one "query", thus an unit of data, which becomes interpreted of the identified programme.

2.2.1.3 HTTP

HTTP ("hypertext transport Protocol") touches down as application log on TCP. Current ones in the use are the versions HTTP 1,0 ([RFC 1945]) and HTTP 1,1 ([RFC 2616]).

HTTP connects a client (typically a www browser) with a server (a Web server). The client sends a request to the server, with which it asks for the transmission of data. Both the addressed server and the identification of the data on the server made over URL.

HTTP made in isolated "Request response" - Cycles, becomes upright obtained between which no connection between client and server. The subsequent Request types are conventional:

- GET: The client asks for the transmission of a file.
Case the addressed resource file, but a programme is not, can complementary still one "query", thus a data sequence, be along-handed. In this case the created called pro-ram an answer file, which is handed back in response.
- POSTS: The client transmitted to the server a list of variables with values. Post office Requests nearly always address programmes on the opposite side. Post office Requests result typically from filled HTML forms.

Other Request types (PUT, DELETE. . .) against it few conventional are.

The HTTP protocol a possible authentication of the user (D. h. the browser opposite the server) with user names and password.

In order to extend HTTP with status informations, D. h. for it to provide that a server details of a preceding Requests of the same Clients "remember" can, it gives it to two common mechanisms. Thus that can implement actual statusless protocol the concept a "session", thus series of Request responseCycles with contentwise connection:

- All pages also hyper+on the left of within a session become dynamic generated.
The session variables become appended thereby to the Query of all internal Hyperlink URLs (for GET Requests) and/or. as post office variables, z. B. in hidden form fields, deposits. When activating the links these data are then sent back by the browser again also to the server.
- An extension of the standard ([RFC 2965] - "Cookies") possible it the server to send in response a value of variables pair to the browser this local stores and then with each Request

to the same server with transmitted.

2.2.1.4 HTML, XML and hyper+on the left of

The “hypertext Markup LANGUAGE” HTML became first up to the version HTML 2,0 ([RFC 1866]) in the frame of the Internet standards defined. In the meantime (with [RFC 2854]) the definition was developed further to the W3 consortium transfered and ([HTML401], [XHTML1], [XML]).

HTML the possible formatted representation of text (z. B. Character size, paragraph formats, tables etc.) as well as merging arbitrary other file formats (z. B. Images, sound, video).

In addition HTML possesses “hyper+on the left of”, thus jump references to other pages, which are in the HTML source text with their URL defined.

HTML and HTTP together form the WWW (World Wide Web). By into the pages the embedded hyper+on the left of to the user the impression, it appears on a group on the part of “would be”, although the HTTP protocol does not know connecting status. Since those can referenzieren URL any www server, the allowed sent combination of HTML pages providing “applications”, which over several servers, possibly world-wide distributed, to extend. By the integration of programmes, which also accept (over HTTP POST OFFICE or one query in HTTP GET) user inputs, the functionality of these “Web applications” arbitrary can be extended and to be copied many common user interfaces of a software functional.

2.2.1.5 SSL and tls

The data transmission in TCP/IP and concomitantly in HTTP made in principle unencrypted and with limited error control. A bad-willing aggressor, the entrance to appropriate routers has, can the data traffic hear and falsify.

In order to prevent this, the company Netscape has an additional protocol layer standardized, which as SSL (see [SSL2]) known is. SSL puts possible on on TCP and puts to the application again Sockets at the disposal (thus again transparent is) for the application during the transmission, however the security of the transmission with various cryptographic methods (symmetric keys, asymetrische with in or reciprocal authentication) like it other down described is.

SSL became received in an extension as TLS ([RFC 2246]) into the Internet standards.

2.2.1.6 https

https, also S-HTTP called, is in [RFC 2660] specified and places the implementation of the

HTTP of protocol over SSL and/or. Tls connections. Algorithms and interfaces to the cryptographic infrastructure are in the common Web server and - browsers implements.

2.2.1.7 firewall

Since the Internet is considered as unschützbarer, public space, the entrances to networks, which contain trusted data, must become corresponding before unauthorized intrusion protected - the comparable gate at a work entrance. The corresponding devices designated one as "firewall". An overview over techniques and terms mediated [RFC 2647].

2.2.1.7,1 Firewall principles

Firewalls use two basic principles:

- Package filters: It concerns particular routers here (see. Portion TCP/IP), which stand between the external and the internal Subnetz and manufacture, reject or reroute only according to certain rules, on the basis of pouring and target addresses of the packets, a connection.
Package filters can convert usually also IP address ("network ADDRESS translation" NAT or "Masquerading").
- Application levelfilters: These filters withdraw opposite the communication partners as receiving station and rate the content of the transmitted data out (z. B. Data types, content, viruses etc.). Depending upon result of the evaluation the content becomes then transparent transfered, disabled, changed or also only the transfer procedure logged.
Apart from security examinations these filters can become also data buffers and then as "proxies" - server designated, whereby the term becomes also synonymous for Application level filter used.
Application level filter must the respective protocol (z. B. Mail, ftp, HTTP. . .) understand, in order to be able to analyze the content.

2.2.1.7,2 Firewall architectures

The Firewalls components become "Firewall architectures" combined. Common basic configurations are:
Simple package filter:
(Internet)----<Package filter>----(internal network)
Routing takes place only according to fixed rules.
It does not take place a contents examination.
Simple proxies:
(Internet)----<Proxy>----(internal network)
It does not take place direct Routing between internal network and Internet.
Only protocols, which are implemented in the proxy, can become transfered.

Three-membered firewall:

EMI6.1
Two-stage firewall:

EMI6.2

With the three-membered and the two-stage firewall zone" between Internet and internal network "demilitarized (English becomes. demilitarized zone = DMZ) as own Subnetz - as it were as Sicherheitsschleuse - provided.

Within the DMZ lower safety requirements than in apply the internal network, many unauthorized accesses from the Internet however already become from the first package filter stage intercepted.

In the DMZ are typically the pro XY servers to the controlling access to the internal network as well as if necessary. the public servers of the organization.

2.2.2 cryptography

Digital cryptography solves bottom application mathematical (usually pay-theoretical) methods various safety requirements of the digital communication during storage and/or transmission, in particular

- Protection before unauthorized access of data by third
- Protection before unauthorized change of data
- Identification and authentication of transmitter and receiver
- examinable commitment and irrevocability of electronic delivered explanations

In the instant invention various established, in the following explained become, method combined.

With the actual achievable security of the methods as well as their influence parameter (key length, organsiatorische measures, physical security etc.) here only in as much one deals as they are relevant to understand the invention. All explanations relate itself on the assumption not corrupted systems.

2.2.2.1 symmetric encryption

The simplest form of the encrypted data transmission used to the en and decryption the same binary sequence as keys. Common methods are in [] and in [3DES] described. An encrypted message can be read only by someone, which has the common key.

Wools several parties communicate confidentially with one another, then either (with use of a common key) only a common confidential communication area or it exists must for all pairs of communications own key be agreed upon.

2.2.2.2 asymmetric encryption

The symmetric encryption requires a confidential connection present first, in order to exchange the key. This cannot become in the typical electronic communication frequent ensured. This limitation go around asymmetric methods. Each party has both parts a part of the full key, must (after specific criteria of the algorithm) fit ("key lock principle").

A message, which with one allot pro rata-hurry encrypted becomes, can become only with the appropriate in each case part of the pair of keys decrypted. The sequence, become applied in which the keys, unimportant thereby (at least with RSA), equally several pairs of keys can become successively applied.

2.2.2.2,1 algorithms

Known algorithms for asymmetric encryption are Diffie Hellman ([RFC 2631] [US-Pat No. 4,200,770]) and RSA ([RSA] [RFC 2313] (as PKCS #1); [US-Pat No. 4,405,829]), DSA as well as algorithms on the basis elliptic curves ([PKCS13]).

So far not differently indicated, relate the subsequent execution on RSA, are however to a large extent more transferable on other algorithms.

2.2.2.2,2 publication IC private key methods

With this method (often also referenziert with PKI - Pubfic key Infrastructure -) each participant at a communication system keeps a key of the pair, while the other to all other participants published becomes.

2.2.2.2 .2.1 coding

To coding a message against unauthorized vintages the encrypted transmitter with it the known public key of the receiver. Only this had the private key appropriate in addition and can decipher the message.

2.2.2.2 .2.2 signature (digital signature)

The transmitter encrypted its message with its own private key. Everyone in the system can

read this message, since the associated keys in the pair by definition public is.

Reading with the public key of the transmitter succeeds however only, if the actual private key of the maintained transmitter became coding used. Bad-willing third, which would like itself to spend abusively than transmitters, but not had its private keys, can not reach this. Thus the authenticity of the transmitter is saved.

The transmitter cannot deny a once delivered message, if it could be deciphered, since only it was in the layer to produce this message.

2.2.2.2 of .2.3 Trust centers

Publication IC key systems require that each communication partner can rely on the authenticity of the public keys used of it.

In the simple case can be made via a previous exchange with the assignee by a safe channel. The required exchange expenditure rises however with the square of the participants and becomes therefore in larger systems expensive.

For this case a "trusted location" (frequent synonyms can: Zertifzierungsstelle, net notary, Certificate Authority, Trust center) intermediate become. The single users exchanges only with this location the public keys over a safe channel. The trust center "signed" the public key of the users and places so their integrity safer.

The distribution of the signed public keys ("certificates") knows z by the user -. B. with a message or by publication in the user circle - take place.

Trust center certificates can be also cascaded ("Certificate chain"), D. h. the integrity examination made indirect over a center, which the respective user opposite not direct, but over an other Trust was authentifiziert center. Analogue ones can certify themselves two first independent Trust centers mutual (CROSS Certificate) and so the circle of users combine.

Details of the usual (standardized) method are in [X.509] described.

2.2.2.2 of .2.4 listing services

The publication of the X-509-Schlüssel can take place in so called "directories" after [X.500], how they are particular for the Internet in [RFC 2459] and [RFC 2510] described.

The common protocol for this is LDAP [RFC 1777], in particular in the current version LDAP v3 [RFC 2251].

These directories are applied as independent server services. They make the search possible of a communication partner for various criteria (among other things also a world-wide unique, hierarchical name for X.500-Konvention, also as DN = "distinguished name" designated). The deposit of X.509-Zertifikaten in LDAP directories is component of the specification.

2.2.2.2 .2.5 Smart Cards

Most sensitive attack place for a PKI is that access unauthorized one to a private key. Since it concerns thereby only a binary sequence, this key can do unnoticed copied and of an aggressor used become (PC maintenance, use in a foreign computer, malignant software on a PC. . .).

In order to prevent this, the private keys on independent apparatuses can become stored, which accomplish the required coding operations, without the private key leaves the apparatus, and which is constructive not at all in the layer to spend the private key. For this the "Smart Card" has itself bottom various suggested configurations in the credit card format established (see [ISO 7816] - 15).

The data sheet of an example product is more bottom [SecurID 3100].

2.2.2.2 .2.6 biometric identification

Smart Cards and similar "Security of token" can be stolen or be left by the assignee in the good faith thoughtlessly. Biometric methods (z. B. ,) Against it the unique identification of a person direct make fingerprint for iris patterns possible on the basis body characteristics.

However the reliability of biometric methods of the integrity of the searching systems at the location of the person which can be identified is dependent (see. [Biometrics]). In the remote authentication an aggressor can pretend the response of a genuine system by a fictitious system, without the person which can be identified is actual present.

It offers itself however to secure the use of private keys on Smart Cards (or other token) with for biometric access supervision so that before each use of the private key a willentlicher must precede act of the assignee (comparisons also [ISO 7816] - 11 and/or. associated standardisation drafts).

2.2.2.3 hybrid method

Asymmetric methods require essential higher cost of computation than symmetric methods due to their complexity. This is continued to intensify by the use of (usually very minimum) token such as Smart Cards, which exhibit a very limited information flow-rate contrary to

modern processors in application computers only.

In many operational areas will therefore various methods combined, in order to optimize the information flow-rate.

2.2.2.3,1 session key

"Session a key" is a random number, with which bottom application of a symmetric method that becomes majority of communication contents encrypted.

The asymmetric method (and if necessary, minimum token) needs to code then only more the session key. This encrypted session key transfered becomes together with (symmetric) the encrypted message. The receiver decrypted first the session key and with this then the remainder of the message.

2.2.2.3,2 hash functions

Hash functions are so called one-way functions, which determine (in the statistical frame) comparatively short, but an unique value (a comparable checksum) from a longer Datensegenz, which becomes often also designated as "finger print" or "hash value". Reverse one is it however not possible to judge from the "checksum" the data themselves.

Common algorithms are known the bottom name MD2, MD4, MD5 (see for this [RFC 1321]) or [SHA]. The application of hash functions is approximately more bottom as HMAC [RFC 2104].

2.2.2.3,3 electronic mail and S-MIME

Coding and marking electronic messages as electronic mail is far common. All common E-Mail programmes have the corresponding technology. The technology and infrastructure developed and can be considered as "sample solution" to the implementation of komlexer cryptographic methods.

The details of the standard "S-MIME" for encrypted transmission of enamels in the Internet are in [RFC 1421], [RFC 1422], [RFC 1423] and [RFC 1424] fixed.

2.2.2.4 Authentifizierungs token

In all distributed computer systems (usually Client serversystems) an authentication of the user at the target computer is required. In the simple case the user (typically with user name and password) at each target system single authentifiziert itself. With larger systems leads to

a significant administration expenditure in the system and to the confusion of the users with many passwords.

Authentifizierungsverfahren with independent test system are since longer known. With these methods exists beside the datarequesting location (z. B a workstation, thus client) and the dataheld location (z. B. a file server) an own Authentifizierungsrechner. The client announces itself first at the Authentifizierungsrechner, only this must in the layer be to make the Identitätspüfung for each user. It created then a "token" or "ticket" after cryptographic methods, which becomes back-transmitted to the client. With this token the client can authentifizieren itself then at various data servers.

2.2.2.4,1 Kerberos

As prototype to the token-based authentication is considered at WITH developed Kerberos, which in its current version V5 as Internet standard ([RFC 1510]) the established is. A Kerberos variant will was verwendt there among other things also in the Microsoft operating system WINDOWS 2000 used and solves prop. guessing eras a mechanism, like it in NT 4, off.

Kerberos of used symmetric keys for each user, which is in the Authentifizierungsrechnern deposited.

2,3 problem definition

2.3.1 concrete object in the medical surrounding field

A physician treated patient and needs in addition data (z. B. Finding, X ray image. . .), of third (z. B. hospital, laboratory or another medical practice) - "data owner" called - stored become.

Various legislation, appointing and rules, confidence expectations of the patients, confidence constellations etc. obligate the data owner to grant only authorized persons access to defined and of the respective persons to dependent area of the data.

Necessary informations, which the data owner needs, in order to meet access decisions, are about:

- Is the requesting person actual physician and if, in which technical field?
- Is the patient, which the data concern, present and has it its agreement issued?
- Is in detail conscious itself the patient over the stored data (it wants z. B. a physician, which it on behalf an insurance examined, obvious that there are extensive data from a heart

hospital)?
- Gives it a special position of trust between the requesting location and the data owner, to z. B. due to special contractual controls?

The application of the required high-safe transmission methods to the state of the art makes excessive demands of the regular involved parties, so that the security of the transmission is to be paged on third out ("safetyobtaining location"), which have however no authority to read the data themselves.

Costing and efficiency criteria require that on pages of the data owner and the safe location the development without direct influencing control of men made.

Beside the pure authentication of the involved persons still other informations of the requirement context required can become, those if necessary. iterative to be queried must.

2.3.2 Verallgemeinerung of the problem definition

The represented solution does not concern the encryption of the transmission paths and included limitation of the data themselves, therefore the use can take place also outside of the medical surrounding field.

Thus the object can become extended:
It is to become a dataprocessing system possible, with a requested data access informations over the context of the intended access, in particular several involved persons, the time, and if necessary. other user-specific informations to obtained. The operation of the access control system is to be able to become thereby by the data retention decoupled.

2,4 natures of the invention

The known safety and Authentifizierungsverfahren will be able to become such combined that to the authentication of a data access several persons must agree, other informations received and the roles various steps in the Authentifizierungsprozess spatial and data technical to a large extent decoupled are.

With will it possible separating the distribution of the responsibility for portions local and organizational and to integrate systems on different platforms.

2,5 industrial applicability

Alone in the health service become predicted, if the communication between several physicians, of specialists an enormous rationalization potential as well as a quality and a service improvement, which treat patients, is improved.

The electronic communication, how it is in many other areas today already usual, could carry for it an important contribution out, failed so far however because of an infrastructure, which remains manageable on the one hand the required safety requirements satisfied and on the other hand for the affected participants.

The described invention can serve as basis for this safety infrastructure.

Other applications result z. B. in the justice, the economic and tax consultation, the personnel switching and - consultation, insurance, the commerce with buyer profiles or financing.

2,6 advantages

Prior solutions on known standards make in each case the authentication for a person possible (z. B. the physician). This has then access to an essential larger volume of data, not only on the respective patients, which can be limited here. Arbitrary complex safety philosophies can be implemented by the transmission of other context data.

An other advantage of the described solution is modularity. Thereby simple existing systems of various data owners and data users with simple interfaces combined can become a safe data exchange network.

2,7 embodiment
see portion 3

2,8 bibliography
to the state of the art:
[3DES]
American National Standards Institute
Tripolarize DATA Encryption Algorithm mode OF operation.
ANSI X9.52-1998; 1998
[Biometrics]
Gaël Hachez, François Koeune and Jean Jacques Quisquater Biometrics, ACCESS control, smart cards: A emergency so simple combi nation
http://www.dice.ucl.ac.be/crypto/publications/Biometrics.pdf
[OF THE]
American National Standards Institute
American national standard for information of system - DATA link Encryption
ANSI X3.106; 1983
[HTML401]
Dave Raggett, Arnaud Le Hors, Ian Yak-generic terms
HTML 4,01 Specification

W3C Recommendation; December 1999
http://www.w3.org/TR/html401
[ISO 7816]
Gisela master
ISO/CInternational Electronical Commission 7816 standards: Status and new Work of item
Giesecke & Devrient, Munich
http://sit.gmd.de/SICA/papers/WS_01/Beitrag_Meister
[PKCS12]
RSA Laboratories
PKCS #12: Personnel information Exchange syntax standard version 1.0; June 24, 1999
http://www.rsasecurity.com/rsalabs/pkcs/pkcs-12/index.html
[PKCS13]
RSA Laboratories
PKCS #13: Elliptic Curve Cryptography standard PROJECT OVERVIEW January 12, 1998
http://www.rsasecurity.com/rsalabs/pkcs/pkcs-13/project_overview.html
[RFC 768]
J. Postel - ISI
User Datagram Protocol
RFC 768; ISI, 28. August 1980
[RFC 791]
DARPA Internet Program Protocol Specification Internet Protocol
RFC 791; September 1981
[RFC 793]
DARPA Internet Program Protocol Specification
Transmission Control Protocol
RFC 793; September 1981
[RFC1034]
Mockapetris, P
Domain Names - Concepts and Facilities
RFC 1034, November 1987
[RFC1035]
Mockapetris, P.
Domain Names - implementation and Specification "
RFC 1035, November 1987
[RFC 1321]
Rivest, R.
The MD5 Message Digest Algorithm
RFC 1321; April 1992
[RFC 1421]
Linn, J.
Privacy Enhancement for Internet electronics mail:
Part I: Message Encryption and Authentication Procedures
RFC 1421; DEK, February 1993

[RFC 1422]
Kent, S.
Privacy Enhancement for Internet electronics mail:
Part II: Certificate Based key management
RFC 1422; BBN, February 1993
[RFC 1423]
Balenson, D.
Privacy Enhancement for Internet electronics mail:
Part III: Algorithms, mode, and Identifiers
RFC 1423; TIS, February 1993
[RFC 1424]
Balaski, B.
Privacy Enhancement for Internet electronics mail:
Part IV: Notary, CO-Issuer, CRL Storing and CRL Retrieving services
RFC 1424; RSA Laboratories, February 1993
[RFC 1510] Kohl, J. and B. Neuman
The Kerberos network Authentication system (V5)
RFC 1510; September 1993
[RFC 1738] Berne R-S Lee, T., Masinter, L., and M. McCahill
Uniformly resource Locators (URL)
RFC 1738; December 1994
[RFC 1777] Yeong, Y., Howes, T. and S. Kille
Lightweight Directory Access Protocol
RFC 1777; March 1995
[RFC 1866] Berne R-S Lee, T. and D. Connolly
Hypertext Markup LANGUAGE - 2.0
RFC 1866; November 1995
[RFC 1883]
DTE ring, S. and R. Hinden
Internet Protocol, Version6 (IPv6) Specification
RFC 1883; December 1995
[RFC 1945]
Berne R-S Lee, T., falling thing, R. and H. Frystyk
Hypertext transfer Protocol - HTTP/1.0
RFC 1945; May 1996
[RFC 2104]
Krawczyk, H., Bell acres, M., and R. Canetti
HMAC: Keyed Hashing for Message Authentication
RFC 2104; February 1997
[RFC 2246]
Dierks, T, and C. Everything
The TLS Protocol version 1.0
RFC 2246; January 1999

[RFC 2251]
M. Choice, T. Howes, S. Kille
Lightweight Directory Access Protocol (v3)
RFC 2251; December 1997
[RFC 2313]
Potash ski, B.
PKCS #1: RSA Encryption version 1.5
RFC 2313; March 1998
[RFC 2396]
Berne R-S Lee, T., falling thing, R. and L. Masinter
Uniformly resource Identifiers (URI): Gene Eric syntax "
RFC 2396; August 1998
[RFC 2459]
Housley, R., Ford, W., Polk, W. and D. Solo one
Internet X.509 publicly key Infrastructure Certificate and CRL of profiles
RFC 2459; January 1999
[RFC 2510]
C. Adam, S. Farrell
Internet X.509 publicly key Infrastructure Certificate management Protocols
RFC 2510; March 1999
[RFC 2616]
Falling thing, R., Gettys, J., Mogul, J., Frysyk, H., Masinter, L. Leach, P. and T. Berne R-S Lee
Hypertext transfer Protocol - HTTP/1.1
RFC 2616; June 1999
[RFC 2631]
Rescorla, E.
Diffie Hellman key Agreement Method
RFC 2631; June 1999
[RFC 2647]
D. Newman
Benchmarking Terminology for firewall performance
RFC 2647; August 1999
[RFC 2660]
E. Rescorla, A. Schiffman
The Secure hypertext transfer Protocol
RFC 2660, August 1999
[RFC 2854]
D. Connolly, L. Masinter
The “text/HTML” Media type
RFC 2854; June 2000
[RFC 2965]
D. Kristol, L. Montulli

HTTP State management Mechanism
RFC 2965; October 2000
[RSA]
R. Rivest, A. Shamir, and L. M. Adleman
A Method for Obtaining digital Signatures and publication IC key Cryptosystems
Communications OF the ACM, v. 21, n. 2, February 1978, pp. 120-126.
[SecurID 3100]
RSA SecurID TM 3100 Smart Card
Secure RSA Cryptographic container for PKI Credentials (Datasheet)
http://www.rsasecurity.com
/products/securid/datasheets/ds3100smartcard.html
[SHA]
NIST
Secure hash standard
FIPS PUB 180-1; April 1995
[SSL2]
Hickman, tilt
The SSL Protocol
Netscape Communications Corp., Feb 9, 1995
[US-Pat No. 4,200,770]
Cryptographic Apparatus and Method ("Diffie Hellman")
[US-Pat No. 4,218,582]
Publicly key Cryptographic Apparatus and Method ("Hellman Merkle")
[US-Pat No. 4,405,829]
Cryptographic Communications system and Method ("RSA")
[US-Pat No. 4,424,414]
Exponentially Cryptographic Apparatus and Method ("bright-one-POH-lie")
[X.500]
Information Technology - Open Systems Interconnection - The directory: Overview OF concepts, models and services
ITU-T Recommendation X.500
ISO/CInternational Electronical Commission 9594-1; 1997
[X.501]
Information Technology - Open Systems Interconnection - The directory: Models
ITU-T Recommendation X.501
ISO/CInternational Electronical Commission 9594-2; 1997
[X.509]
Information Technology - Open Systems Interconnection
The directory: Authentication framework
ITU-T Recommendation X.509
ISO/CInternational Electronical Commission 9594-8; 1997
[X.520]
Information Technology - Open Systems Interconnection - The directory: Selected of

attributes of type.
ITU-T Recommeridation X.520
ISO/CInternational Electronical Commission 9594-6; 1997
[X.680] Abstract Syntax Notation One (ASN.1) - Specification OF basic notation
ITU-T Recommendation X.680; 1994
[XHTML1]
Steven Pemberton et. aluminium
XHTML 1.0: The Extensible hypertext Markup LANGUAGE:
A Reformulation OF HTML 4 in XML 1.0
W3C Recommendation, January 2000
http://www.w3.org/TR/xhtml1
[XML]
Tim Bray, Jean Paoli, C. M. Sperberg McQueen, Eve painter
Extensible Markup LANGUAGE (XML) 1,0 (Second edition)
W3C Recommendation; 6 October 2000
hftp: //www.w3.org/TR/REC-xml

3,1 preface

The described embodiment is based on the concrete object in the medical context (see. Explanations to the patent request) and used therefore the corresponding terms “physician”, “patient” etc. At the basis located object consists of it, the physician access to confidential data of the patient, which it straight treated to grant only to this patient and only in a scope, how it corresponds to its condition-legal permission and the consent of the patient (see. Claim 1).

Possible extensions and variants of the method are partial (in italics printing) in the text as well as in the last portion described, result however in particular from the claims.

3,2 architecture

The components involved at an overall system are outlined in the drawing 1.

It becomes spoken for the three essential components - requirement place, access supervision and data retention - always in the singular one. In a developed system natural instances several of all these locations can occur, the other also with one another networked (z. B. over HTML links) to be can.

3.2.1 work station to the access request

At the workstation of the physician is a PC with a standard Web browser. It becomes assumed that that access to the data preferably over HTML/HTTP made, since can become

achieved thereby a simple integration and standardization.

Complementary one can be present at the medical practice also own practice one agent system ("PMS"), either over the browser or independent, but naturally also over HTTP/https data after release to call up knows. The integration of the PMS is however insignificant for the understanding of the instant invention.

The reliability of the PC and the practice software is subject to the control of the physician.

3.2.2 key maps of the users

Both physician and patient have a Smart Card with private key put down there and integrated Kryptoprozessor (according to claim 7 and 8).

For physicians there is already for it an established standard ("health professional card" - HPC), these defaults the satisfied.

For the patients there is no defined standard. The card of the patient is provided with a finger mark reader, that must become triggered before each coding action and ensures that before each key use an explicit, personal expression of will of the patient is present (claim 9 and 10).

The work station of the physician must be with appropriate readers provided, in order to head for the Smart Cards (simultaneous or successively).

3.2.3 access control system

The access control system ("ACCESS management stroke") is spatial and organizational independent of medical practice and database.

It is connected over a firewall with the Internet.

It has a database of the public keys of all registered physicians as well as all certification bodies, which are authorized by patients to the registration (ACCESS directory).

This database can be because of the location of the access board of control or over appropriate directory protocols (z. B. LDAP) totally or partly by other locations to be imported (see. Claim 21 FF).

Extension

Become - different of the image - multistage certificate chains used (see. Claim 18), is sufficient it for the searching location to reproach the certificates of the lowest planes of the used chains. In this case the complete certificates must inclusively if necessary. all intermediate certificates on the smart cards to authentifizierenden persons deposited its and as component of the Authentifizierungsantrages with transfered become (claim 20).

The access board of control represents the most sensitive system in the safety chain and is therefore in independent high-safe area of a specialized Dienstleisters ("ACCESS security more provider").

Extension

All procedures know - z. B. to the preservation of evidence in controversies - along-logged become ("ACCESS log").

Extension

The access board of control can already reproach informations, where which data are over patients a stored ("location directory")

3.2.4 data stores

The database with patient data becomes as existing assumed.

The interface for main line train reef should come as close ones as possible to the request of browsergestützter systems, which for example by the application of the XML version of the international patient data standard "hl7" achieved can become.

The data store is not direct from the Internet more achievable (claim 39).

3.2.5 release system

The release system ("access control server") is a rear firewall (claim 39) at the location of the data owner, z. B. an hospital ("hospital or OTHER of maintainer OF health information services").

In the example assumed becomes that the database supplies informations in the XML format, which can be read reduced by the common present browsers only. In this case the release system can make a translation ("XSLT Processor") in standard HTML. In addition, XML data direct can be through-handed (after made release) or, if the database can supply HTML format, also this can be passed on after examination. As a result of these variation options wide possibilities of adaptation arise to present systems.

For the implementation each common programming environment can become used. Java Servlets offer for example the required HTTP interfaces and are open for the important network, Krypto and XML libraries.

That access to the data store made typically again over a package filtering to IP and haven plane (thick black line with holes), so that the release system in a DMZ between two package filters is (see. "State of the art/firewall" as well as claim 39 and 40). Alternative one, but with same functionality, the made communication between firewall and database over another protocol than TCP/IP, so that a direct Routing becomes from the Internet efficiently prevented.

The release system receives its access control information from the database (claim 30 FF, in the image indicated with the thick double arrow), whereby the accurate implementation depends on how these informations are present. A simple possibility consists of the fact that the access control information as well as the data (claim 32) is, approximately in the HTML header deposited as Meta day (claim 33) or as specific fields in a XML format (claim 34).

3.2.6 data transmission

The data transmission made in the example exclusive over the Internet (see. Claim 2), thus first uncertainly.

All connections become over SSL, thus encrypted, realized (claims 16, if necessary. 21, 26/27, 36). Made always a alternate authentication (thus both opposite server client and client opposite server), in order to grant a highest possible protection opposite aggressors.

The flows are so designed that the simple HTTP protocol with Request responseCycles is sufficient. Thus the standardized https protocol (HTTP over SSL) can become used at all connections (claims 17, 27, 36).

Extensions and variations of network minutes are more conceivable in this place, promise however no functional advantage.

3.2.7 Trust centers

In the described flow are series of asymmetric pairs of keys in the use, at least:

- Keys of the physician on the HPC (claim 1)
- Keys of the patient (claim 1) on its biometrically saved (claims 9, 10) card
- SSL client keys of the physician workstation (claim 16 and 35)

- SSL server keys of the access control system (claim 16 and 26)
- SSL server keys of the release system (claim 26 and 35)
- SSL client keys of the access control system (according to claim 24 and 26) and/or the release system (according to claim 25 and 26)

These keys become naturally of a Trust center as specialized Dienstleister generated and/or acknowledged in their authenticity (claim 10). To what extent here a single or several Trust center used become, and whether these organizational at one of the represented locations, z. B. the access board of control, attached are, is not from technical view not from concern.

3,3 flow from user view

3.3.1 request software

If the physician takes up its treatment, or activated it loads an appropriate "request software" (z. B. an Java applet executable in the browser; "Authorizing applet" in the image), on its computer the before-installed is or which it from a trusted source (z. B. also the access board of control) knows relate.

3.3.2 release request

The request software required now after the identity proofs, thus for instance the Smart Cards of physician and patient. The final agreement (according to claim 1) requires still the release of the key on the cards, z. B. by a password with the HPC and by the fingerprint with the biometric Patientenkarte.

After mailing the release request (according to claim 3) to the access board of control this announces either a Authentifzierungsfehler or a one hyper+left to the next step.

The screen departure represented in drawing 2 on page 52 shows a pilot version such release applet, replaced with which the Smart Cards is by binary sequences, which become over the Windows intermediate file into corresponding windows inserted ("paste doctor's/patient's key here").

The release made in the pilot version by passwords, which in the image with the patient already made is ("open") and for the physician still one queries ("please of enter passwords")

3.3.3 data selection

In the example assumed becomes that the access board of control already has a list of data available to the patient. In this case a corresponding list can become as HMTL page also hyper+on the left of shipped to the workstation of the physician, whereby hyper+on the left

of on the respective release servers refer.

Physician and/or patient select (if necessary. common) the data which can be called up out ("other context information" according to claim 1).

3.3.4 data fetch

Ideally the opened system behaves opposite the physician like a set of HTML pages, it can thus in the inventory of the patient data with its Web browser "surfen" (claim 41 FF) and if necessary. important informations into its own practice data system "downloaden".

Extension

With appropriate data structure with it also cross reference between various volume of data can occur. If necessary. the system will require for a renewed authentication, if for instance the area of another access board of control is or the patient or other right ones (z will enter large release-right for particularly trusted data. B. Write access) to give is.

3,4 cooperation of the cryptographic components

The required cryptographic flows are to run off with successful authentication to a large extent in the background. Only with a Authentifizierungsfehler error messages are to be so far expressive that operating errors can be repaired. However error messages may not reveal valuable informations to potential aggressors or to already trusted data (and/or.) abandon their existence (wrong would be z. B. "You are not authorized, the volume of data of the craze welfare clinic to access").

3.4.1 keys

The format of the keys corresponds to the X.509-Standard, as it becomes understood of common Internet browsers. (Example: see drawing 3)

The keys for https must be able to become thereby direct by the browser understood. For the Smart Card key is this not necessarily necessary, since they are addressed via the Authentifizierungssoftware. The use of standardized formats possible however the access to present, tested software libraries to the generation and processing of the cryptographic data.

A pair of keys, which from a browser in the PKCS#12-Format ([PKCS12]) is exported, presents themselves first as follows:

EMI25.1

The essential components are the private key ("BEGIN/END RSA PRIVATE KEY") as well as the X.509-Zertifikat with the public key ("BEGIN/END CERTIFICATE"). Both components are in the representation base-64-kodiert, which serves however only the transferability of binary data and not the Zugriffssicherheit. The other indications serve only the internal organization of the PKCS-12-Formates.

This format corresponds essentially also to the internal representation on a Smart Card.

The certificate, that the authenticity of the key by Trust center acknowledged, has (after base-64 decoding) the subsequent structure (after [X.509]).
EMI26.1

- "Subject" is thereby the name of the person which can be identified
- "more issuer" the Trust center, which the authenticity acknowledged (see. Claim 10a).
- Validity (effective date) and serial number as well as version and algorithms are other organization components after X.509
- The public key ("RSA publicly key") is essential component of the certificate
- The signature (initiated with the indication of the algorithm), those the authenticity of the key acknowledged, locks the certificate.

The private key is in a password-protected "key Bag" accommodated, D. h. additional to the base-64-Dekodierung is still another decryption with the password required.

Only after opening the "key the internal structure of the private RSA key opens Bag" by password input (or fingerprint), how it is required to the use:

EMI27.1

For keys, which are deposited on Smart Cards, this structure of the private key is from the outside not accessible (also not after release). All data which can be coded must become, become into the Smart Card transfered there (after release) encrypted and the Smart Card selected.

3.4.2 Authentifizierungs applet

The Authentifizierungs applet takes over the subsequent functions:

- Providing random generated session a key (claim 4 and 11)
- Determining the current system time (for claim 4)
- Determining the identity of physician and patient (claim 1 - z. B. "Distinguished Names" after X.500 or particular physician/patient indices)

- Queries of the agreement of physician and patient (claim 1)
- with distribution of the agreement: Encryption session of the key with the respective private key of physician and patient (claim 5 and 6 as well as 12)
- Assembly of the components to a session Request (according to claim 3 FF)
- Marking the session Request with (unencrypted) the session key (claim 13)

Extension:
If the https Clienf key in the session Request is to become transfered, then the applet must call these up from the browser (claim 14 FF, in particular 17)

Extension:
If necessary still other informations become the specification of the context, like indicated in claim 1 mentioned,

Extension:
The X.509-Zertifikat of a person involved at the authentication (or several persons), if necessary. also associated certification chains, can likewise become in the request with received (claim 20). In this case only the corresponding root certificate needs to be reproached with the access control system (see. Claim 19). Thus will the responsibility, the authority of a person, the system general to use to examine of the access inspection station to the Trust center discharged.

3.4.3 session Request

The created session Request (S. Claim 3 FF) has the subsequent structure in the example (without X.509 of certificates according to claim 20):

EMI29.1

This structure knows z. B. in ASN.1 (see [X.680]) shown will become, in base 64 encoded in such a way and then as Query to URL an appended and via HTTP (s) to the access control system transfered.

3.4.4 Authentitätsprüfung by the access control system

The access control system decoded query:

EMI30.1

From it results the ASN.1-Struktur, which reveals the components of the session Requests (see. ASN.1-Struktur like indicated above):

EMI31.1

Now the informations are present, in order to make the examination of the authenticity:

- from the identity information from physician and patient as well as their Zertifizierern become the corresponding certificates determined
- Over serial number and finger print of the certificates a first authenticity test becomes made (claim 18)
- The certificates contain the respective public key
- that encrypted present session key becomes with the two public keys of physician and patient decrypted (claim 12):
Then and only then if both physician and patient with the proper private key worked, leave themselves so to the original session key restore
- It becomes the hash value of the session Requests formed and with restored session the key encrypted. If the result with the transmitted value ("Bag seal") is identical, serves as evidence for a correct authentication (claim 13)

In such a way restored session key if necessary other used can become, in order to code the other communication, so that only the authorized parties can participate in it (claim 15).

Extension:
The access control system can call the SSL key up of the Clients from the Netwerksoftware, if this information is not component of the session Requests. Thus clientseitig the need is void that the applet must access the https key. This the again simplified use of Standardbrowsern on Clientseite.

3.4.5 release servers

The decrypted session key, the SSL identity of the PC in the medical practice and the other informations of the session Requests become transmitted to the release server (according to claim 23). For this z can. B. the access control system a https connection to this develop (see. Claim 24, 26, 27). The release server stores the informations, in order to be able to evaluate it for the case of a data fetch.

Thereupon the transmitted access control system a success message to the browser with the physician, those naturally one hyper+left on the release server (and/or. ever contains a link on each server, if volume of data at various locations is present). In addition the links (according to claim 28 and 29) can contain of Query variables, which serve for the other specification of the required data (z. B. Name of the patient to avoid around mistakes with short successive query).

By activating the links in the browser (claim 41 FF) the physician system sends now HTTP

(s) - a Request to the release server. This calls the desired data up from the database and receives from this (if necessary. also before) the prerequisites required for the access (claim 30 FF). It compares these prerequisites with the stored data from the before transmitted session Request (claim 30).

The other the determined release server the SSL identity of the physician PC and compares it with from the access control system the transmitted (claim 35, 36). With the fact prevented becomes that an unauthorized user with one recorded access sequence, which he do not analyze but 1: 1 to show knows, data access receives ("replay attack").

If all examinations are successful, the release server transmits the requested data as HTTP (s) - response to the physician PC. This response can other hyper+on the left of to other data on same or another system contained (claim 41 FF). If required for a retrieval certain contents of one are URL query, these are passed on in response ("state management" in the HTTP protocol, see. also claim 28 and 29).

3,5 additions and extensions

Important variations of the invention, which are not in the embodiment or only andeutungsweise detected here, become in the following still mentioned.

3.5.1 complexes encryption in the data transmission

In the described example the made transmission between releasing location over https, thus encrypted with the SSL client key of the physician PC. This key is usually deposited on the computer in a file and is thereby unauthorized accesses z. B. at the computer administration exposed ("one RK the end attack"). This key does not offer thus by far the security like the Smart Card based keys to the personal authentication.

Alternative keys, which can repair this lack, are in claim 37/38 described. In particular the session key would come for this into question. Most of these solutions have however the disadvantage that no more Standardbrowser used to become clientseitig to be able.

3.5.2 writing data access

The prior descriptions of the embodiment relate itself partial implicit on reading access.

The flows for writing access (data put on, change, delete, right ones change) are to a large extent identical. Only the release server and the communication with the database corresponding matched must become. As communication protocol with client can become further HTTP (s) used, by forms and Post office Requests a data input possible.

3.5.3 listing services for certificates

The described embodiment does not deal with from where the certificates come, which become used for the Authentitätsüberprüfung. Apart from the transmission with session Request according to claim 20 are the variations in claim 21 and 22 stated.

A meaningful possibility would about be, if the output of the Smart Cards of a Trust center made, that not only the identity of the assignee, but also large prerequisites to the participation at the system (z. B. with a physician the technical permission) examines and holds. These informations can then - together with the certificate - of this Trust center over LDAP (if necessary. over a saved connection) the access control system transmitted become.

With a removal of the system several independent locations can take over this certifying (z. B. Health insurance company branches for patients). In this case a multistage Zertifzierungsverfahren is recommended, how it is in [X.509] provided and in claim 18 FF mentioned.

3.5.4 directory of the available data

The described implementation assumes in the long run only the dataheld system possesses detailed informations, which data to a specific context for the order.

In addition, this information can become differently over the single system components (access supervision, release, several dataheld locations, dedicated directories) distributed. Also a combination with other volume of data (listing service after proceeding portion, access check list) is more conceivable.

The detailed variation options of the data base Design result from practical and safetypolitical considerations and go beyond the frame stressable in this patent.

3.5.5 iterative agreement to the data release

In the drawing to the overall system a “Selection is key” indicated, which becomes used, if the patient is to give explicit agreement to the disclosure of a limited partial selection from all available informations. In the other explanations from reasons of clarity one did not continue to enter on that.

Here it concerns context-specific informations (according to claim 1), which become determined by several requirement cycles (according to claim 41).

The Selection key takes over thereby the role session of the key; as it were by iteration according to claim 41 a new context according to claim 1 is opened.

3.5.6 agency of persons

Claim 45 mentioned various agency constellations. Examples for this can be:

- a physician, an assistant call up data do not separate
- Patients will represent from educate-authorized or a guardian
- A "emergency entrance" the possible access to data of patients without consciousness
- Access rights become not a person, but an organization granted
- Access keys can in a software, z. B. the practice software of the physician, deposited its
- Applications in other one than here the exemplarily represented context can contain other agency possibilities

Which agency possibilities allowed are are a question of the security politics.

3.5.7 determination of a security politics

Many decisions over the implementation can be met not after technical considerations on the search for a "optimum security", but develop by consideration between safety engineering, legal requests, compatibility with existing systems or operability. Even subjective confidence of "feelings" must be included here with. These considerations extract themselves naturally from the technical nature of a patent, why in this description such decisions and variants regular open are left.

Constructing on the here described backbone adjustments can become to a predetermined security politics - with given requests - by an experienced person skilled in the art made.

Result Page

Notice: This translation is produced by an automated process; it is intended only to make the technical content of the original document sufficiently clear in the target language. This service is not a replacement for professional translation services. The esp@cenet® Terms and Conditions of use are also applicable to the use of the translation tool and the results derived therefrom.

1. Method for access price increase on electronic stored data in distributed heterogeneous environments, characterized by the fact that
the release of the data access by several persons made
a third location for release examination between data fetch place and data memory place is switched on
for the examination of the authenticity of the release giving persons cryptographic methods with public and private keys used become
the context situation of the persons in the frame of the service request also into the scope of the issued release to flow can.

2. Process according to claim 1, characterized by the fact that
for the data transmission of appropriate network minutes used to become to be able,
for the data transmission the Internet minutes family (in particular IP, TCP, UDP) used to become to be able,
for the data transmission the Internet used will can.

3. Process according to claim 1, characterized by the fact that for each procedure, becomes requested with which a release
a particular digital release object ("Authentifizierungsantrag") the communication of the involved systems among themselves created becomes
the release object an unique feature of the Authentifizierungsvorganges contains
the release object other data over the Authentifizierungskontext contained can

4. Process according to claim 3, characterized by the fact that
the release object a random generated or otherwise than unique valid digital keys to the identification of the Authentifizierungsvorgangs contained can
the release object a time stamp of the Authentifizierungsantrages contained can
the release object indications over the temporal scope of the authentication contained can

5. Process according to claim 1, characterized by the fact that the persons involved at the Authentifizierungskontext are identifziert by asymmetric digital pairs of keys

6. Process according to claim 5, characterized by the fact that one of the subsequent methods for the asymmetric digital keys becomes used:
RSA
DSA
elliptic functions

7. Process according to claim 5, characterized thereby that the private key of a person on a physical independent unit, involved at the authentication, becomes held, those
of the person entrained will can
of the system, which becomes used in the data fetch place the request of the data release, separate will can
with different systems to the request of the data release used will can
the required coding operations make can, so that the private key of the person does not have to become transfered to the system the request of the data release

8. Process according to claim 7, characterized by the fact that this independent unit is a commercial Smart Card (integrated switching circuit, incorporated into a plastic housing in the cheque card format) with Kryptoprozessor

9. Process according to claim 5 to 8, characterized by the fact that the private key is protected by a biometric feature before unauthorized use

10. Process according to claim 9, characterized by the fact that as biometric feature or the several subsequent ones of an used to become to be able:
individual fingerprint
individual iris patterning
individual face courses
individual language
genetic patterns
Pattern from the gene expression, in particular RSA and proteins

11. Process according to claim 1 to 10, characterized by the fact that for the identification of the Authentifizierungskontextes an unique binary sequence becomes as "session key" used

12. Process according to claim 11, characterized by the fact that the session key with private keys of persons involved at the context becomes encrypted

13. Process according to claim 3, 11 and 121 characterized by the fact that the integrity of the Authentifizierungsantrages becomes ensured by the fact that the entire request or parts of it becomes with session key or a binary sequence derived of it the digital signed

14. Method after all claims specified so far, characterized by the fact that the system, which becomes the request of the data release used is component of the Authentifizierungskontextes

15. Process according to claim 14, characterized by the fact that
the requesting system opposite the searching system by an independent asymmetric pair of keys identified will can
the communication between requesting system and searching system encrypted to take place can

16. Process according to claim 15, characterized by the fact that the communication between requesting system and searching system can be made by a variant of the protocol SSL or tls ("secure Socket Layer")

17. Process according to claim 16, characterized by the fact that the authentication of the apparatus used opposite the searching location and the encryption of the data transmission the protocol becomes https ("HTTP of over SSL")

18. Method after the claims specified so far, characterized by the fact that the examination of the validity of authenticity statements on the basis one of these possibilities made:
one with the searching location of deposited public key as counterpart to the private key of the too authentifizierenden participant
the electronic certificate of a trusted instance ("Trust center"), whose public key is present with the searching location
the electronic certificate of a trusted instance ("Trust center"), whose authenticity of a chain consists of certificates of authenticity, whereby at the beginning of the chain an instance stands, whose public key is present with the searching location

19. Process according to claim 18, characterized thereby that for authenticity examination the methods used become, how they are in ISO X.509 fixed

20. Process according to claim 18 and 19, characterized by the fact that to the Authentifikation required additional information (z. B. X.509-Zertifikate, certificate chains or comparable data) together with the release request transmitted to become to be able

21. Process according to claim 18, 19 and 20, characterized by the fact that in a database at one of the subsequent locations are the public key required for authenticity examination: the searching location
within the immediate, controllable safety sphere of the searching location
a public available location, to which from the searching location a unverfälschbare data connection consists

22. Process according to claim 21, characterized by the fact that the transmission between the searching location and the database through one of the subsequent standardized protocols made
ITU-T recommendation X.500 FF.
Lightwighted Directory Access Protocol (LDAP)

23. Method after one claims specified so far, characterized by the fact that
the examination of the authenticity of the release of giving participants via another location to take place can than that, which gives the data to free
the release of the data via another location to take place can than that, which has the data stored

24. Method after 23, characterized by the fact that
the searching location to the releasing location an appropriate record transfers, the releasing location the evaluation of the context possible ("push session Request")
this record at the releasing location stored will can, until a request of the calling up location made
and/or due to the release data record data to the calling up location transmitted to already become to be able

25. Method after 23, characterized thereby that the releasing location of the searching location calls an appropriate record up, the releasing location the evaluation of the context possible, as soon as a request becomes directed to the data release to it ("pull session Request")

26. Process according to claim 23 to 25, characterized by the fact that
the communication between releasing and searching location with mutual cryptographic authentication to take place can
the communication between releasing and dataheld location with mutual cryptographic authentication to take place can
the communication between releasing and searching location encrypted to take place can
the communication between releasing and dataheld location encrypted to take place can

27. Process according to claim 26, characterized by the fact that
the communication of the designated systems over SSL (or tls) made
the communication of the designated systems over https to take place can

28. Process according to claim 23, characterized by the fact that instead of or complementary to a direct communication between releasing and searching location the searching location an appropriate, cryptographic date signed of the searching location ("ticket" or "token") to the requesting location transmitted, which proves the correctness of the authentication and with then the requesting location opposite the releasing location prove itself can

29. Process according to claim 28, characterized thereby that this token over appropriate HTTP doing management technologies becomes transfered, in particular
in the browser of the requesting location stored variables' contents ("Cookies")
from Requestzyklus to Requestzyklus passed on URL Query and/or. HTTP post office variable of contents

30. Method after claims mentioned, characterized by the fact that
the releasing location a "access check list" had, which indicates, who bottom which prerequisites access with which authority to which data has
the content of the access request, in particular also the corresponding informations over the access context, compared with which becomes defaults from the access check list and from it the been entitled access rights derived become

31. Process according to claim 30, characterized by the fact that the releasing location calls the access control information up if necessary from the dataheld system

32. Process according to claim 30, characterized by the fact that the dataheld location the access control information direct with the requested data - still before the authorization check - to the releasing location transmitted

33. Process according to claim 32, characterized by the fact that
the dataheld system the requested response to the releasing system in the HTML format transmitted
the access control information as specific in the browser disturbing or from the release system to those which can be removed of HTML day transmitted does not become

34. Process according to claim 32, characterized by the fact that
the dataheld system the requested response to the releasing system in the XML format transmitted
the access control information as particularly defined XML elements or - attributes transmitted

35. Method after claims mentioned (in particular 14 to 17), characterized by the fact that that access to approved data only from the system to take place can, which has the release requirement created
the Authentifizierungsinformationen access of the requiring system of the Authentiztät examining system to the releasing system with transmitted becomes
this Authentifizierungsinformationen network-specific data (z. B. IP address, DNS name) contained know
this Authentifizierungsinformationen of components or unique features of a cryptographic pair of keys contained can

36. Process according to claim 35, characterized thereby that
the searching location to the releasing location the SSL client key of the requesting location to convey can
the releasing location with the requesting location over SSL or tls (if necessary. as https) to communicate can

37. Method after claims mentioned, characterized by the fact that the communication between the releasing location with the requesting location on network and/or data plane with (among other things) or the several subsequent keys an encrypted can be authentifiziert and/or:
Session key of the context-based request
Pair of keys or the several persons involved at the context of the request
Pair of keys of the system used to the request
Pair of keys of the releasing system

38. Process according to claim 37, characterized by the fact that used instead of a direct encryption also one can become in cryptography known hybrid procedures

39. Method after claims mentioned, characterized by the fact that
releasing and dataheld location in a Firewall topology incorporated are
here the dataheld location in the protected internal area and the releasing location in the "DMZ" ("demilitarized zone") the firewall to lie can

40. Process according to claim 39, characterized by the fact that the releasing location is as "Application level proxy" on layer 7 of the OSI reference model realized

41. Method after claims mentioned characterized by the fact that
the release of the data in several requirement cycles to take place can
the release requesting persons thereby other context information to deliver subsequently know
the release giving location informations over available data and/or required other context information to the release requesting location to send can
by repeated Cycles the scope of the approved data extended or to be concretized can

42. Process according to claim 41 characterized by the fact that
the switch between the Cycles hyper+on the left of, how they are for instance known from the WWW, used to become to be able
this hyper+on the left of static fixed or dynamic from the involved systems generated to become to be able

43. Process according to claim 41 and 42, characterized by the fact that the Hperlinks can be contained in documents the subsequent structure:

Hypertext Markup LANGUAGE (HTML)
Extended Markup LANGUAGE (XML)

44. Process according to claim 41 to 43, characterized by the fact that the transmission becomes used during the requirement cycles a variant of the Internet protocol HTTP (in particular also https)

45. Method after claims mentioned, characterized by the fact that
to the location of natural persons also different legal persons to step can
Persons also different represented can
the role by persons, which act in the own name or in agency, of data technical systems to be taken over can, which show the same behavior, and whose function of it is dependent within the described method that the person represented by the system this action tell-did by an expression of will to the system opposite.